ART 34 AMDT

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, characterized by
   a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
   b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
   c) sending the secure message from the first computer to the intermediate computer,
   d) using said destination address and the unique identity to find an address to the second computer,
   e) substituting the current destination address with the found address to the second computer,
   f) substituting the unique identity with another unique identity,
   g) forwarding the secure message with substituted current destination address and substituted unique identity to the second computer.

2. Method of claim 1, characterized in that the secure message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.

3. Method of claim 1, characterized in that the secure forwarding of the message is performed by making use of the SSL or TLS protocols.

4. Method of claim 2, characterized in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.

5. Method of claim 2, characterized in that a preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol.

ART 34 AMDT

6. Method of claim 5, characterized in that the automated key exchange protocol used for the preceding distribution of keys for forming the IP Sec connection is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and by means of a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. Method of any of claims 2, 5 or 6, characterized in that the message that is sent from the first computer in step c) is a packet and contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, the unique identity, and other security parameters.

8. Method of any of claims 2, 5 or 6, characterized in that that the IPSec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include one or more sequence numbers.

9. Method of any of claims 1 – 8, characterized in that the matching in step d) is performed by using a translation table stored at the intermediate computer.

10. Method of any of claims 1 - 9, characterized in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).

11. Method of any of claims 1 - 10, characterized in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.

12. Method of claim 11, characterized in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer.

ART 34 AMDT

13. Method of claim 12, c h a r a c t e r i z e d in that a reply to said request for registration is sent from the intermediate computer to the first computer.

14. Method of claim 12 or 13, c h a r a c t e r i z e d in that the request for registration and/or reply is authenticated and/or encrypted by IPSec.

15. Method of any of claims 4 -14, c h a r a c t e r i z e d in that the key distribution for the secure connections is established by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

16. Method of claim 15, c h a r a c t e r i z e d in that the key exchange distribution is established by
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer,
using the translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

17. Method of claim 15 or 16, c h a r a c t e r i z e d in that the modified IKE protocol between the first computer and the intermediate computer is modified by transmitting the IKE keys from the first computer to the intermediate computer in order to decrypt and modificate IKE packets.

18. Method of claim 15 or 16, c h a r a c t e r i z e d in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets is done by the first computer with the intermediate computer requesting such modifications.

ART 34 AMDT

19. Method of claim 17, characterized in that the address is defined so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

20. Method of any of claims 1 -19, characterized in that the secure message is sent using IPSec transport mode.

21. Method of any of claims 1 -19, characterized in that the secure message is sent using IPSec tunnel mode.

22. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, characterized in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have translation tables to perform IPSec and IKE translation.

23. Network of claim 22, characterized in that the translation table for IPSec translation comprises IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

24. Network of claim 22, characterized in that the translation tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

25. Network of claim 24, characterized in that both partitions of the mapping table for IKE translation contains translation fields for a source IP address, a destination IP address, initiator and responder cookies between respective computers.

26. Network of any of claims 22 - 25, c h a r a c t e r i z e d in that there is another translation table for IKE translation containing fields for matching a given user to a given second computer.